IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

APPEAL NO:

In Re Application of: Martin J. PAGEL

Confirmation No.: 1033

Serial No.: 09/608,123

Filed: June 30, 2000

For: EVIDENCING INDICIA OF VALUE USING SECRET KEY CRYPTOGRAPHY

SUPPLEMENTAL APPEAL BRIEF

Stephen G. Sullivan
Attorney for Appellants
Strategic Patent Group
P.O. Box 1329
Mountain View, CA 94042

TOPICAL INDEX

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In Re Application of:	Date: November 3, 2006
Martin J. PAGEL	Confirmation No.: 1033
Serial No: 09/608,123	Group Art Unit: 2136
Filed: June 30, 2000	Examiner: Colin, Carl G.

For: EVIDENCING INDICIA OF VALUE USING SECRET KEY CRYPTOGRAPHY

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

Appellant herein files an Appeal Brief drafted in accordance with the provisions of 37 C.F.R. §41.37 as follows:

I REAL PARTY IN INTEREST

Appellant respectfully submits that the above-captioned application is assigned, in its entirety to Stamps.com of Los Angeles, CA.

II RELATED APPEALS AND INTERFERENCES

Appellant states that, upon information and belief, he is not aware of any co-pending appeal or interference which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III STATUS OF CLAIMS

Application Serial No. 09/608,123 (the instant application), as originally filed, included claims 1-31. Claims 28-31 are presently pending and stand rejected. In response to the Office Action dated February 9, 2004, claims 1, 2, 4, 10-18 were amended. In response to the Final Office Action dated November 16, 2004, claims 1-27 were canceled. In response to the Examiner's Advisory Action dated April 28, 2005, an Amendment was submitted with a Request for Continued Examination (RCE) in which claim 28 was amended. Rejected Claims 28-31 are on appeal and all applied prospective rejections concerning Claims 28-31 are being appealed herein.

IV STATUS OF AMENDMENTS

All submitted amendments have been entered. No amendment has been submitted in response to the Final Office Action dated March 7, 2006.

V SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 28 recites a method and system for dispensing and evidencing indicia by a postage indicia generating device in a system having a plurality of indicia generating devices that have been divided into n groups. As shown in FIG. 2, in a preferred embodiment, the system includes a key distribution center (KDC) 24, a plurality of postage generating devices (PDGs) 14, and multiple USPS distribution centers 20 (Specification, page 6, lines 20-22). The plurality of postage generating devices (PDGs) are divided into n groups corresponding to different geographic designations (e.g., zip codes), and a set of verification keys, V_i, is assigned to each PGD group, where each verification key in the set is encrypted as a function of one of the corresponding destination regions (See page 7, lines 13-19; and page 8, lines 12-13, for example). The key distribution center also assigns a set of key ID's 23 to each PDG group, where each key ID in the set is associated with one of the assigned verification keys and is encrypted as a function of the same destination region used to encrypt the corresponding verification key (See page 7, lines 20-23; and page 9, line 9 through page 10, line 8, for example). After assigning the verification keys 21 to the PGD groups 26, the KDC 24 distributes to each distribution center the sets of verification keys 21 and key ID's 23 that were encrypted as a function of the corresponding destination region (See, page 8, lines 9-13; and page 10, lines 9-19, for example).

The process recited in claim 28 performed by the indicia generating devices begins in step (a) when the indicia generating devices receive a master secret key K and a secret key K_i from the distribution center over a network after manufacture, and store the master secret key K and the secret key K_i in the PGD. Support for receiving

the master and secret keys can be found in the Specification on page 10, lines 22-23). Support for receiving the keys "from a distribution center over a network after manufacture" is inherent in the specification, see for example, pages 1-3 and 6 -8. In particular, page 7, lines 3-5 describe that the "…the key distribution center 24 distributes the cryptographic keys to the PGDs 14 and to the distribution centers 20 via a telecommunications network." Since FIG. 2 (and FIG.1 to which FIG. 2 is compared) show the PGDs 14 coupled between a distribution center and a distribution center, the distribution of the keys over the network clearly occurs after the PGDs have been manufactured. Support for the master secret key K and the secret key K_i being stored in the PDG is inherent in the Specification, particular the paragraph on page 10, line 20. Because a user request to generate the indicia may occur well after the PDG receives the master secret key K and the secret key K_i from the KDC 24, it is clear the PDG may store the master secret key K and the secret key K_i after receipt.

In steps (b) and (c), in response to receiving a request from a user to generate an indicium for a mail piece destined for a particular destination *Dest*, an indicium is generated, and a verification key V_i^{Dest} is computed as a function of the secret key K_i and the destination (See page 10, line 23 through page 11, line 5, for example). In step (d), an encrypted key ID I_i^{Dest} is computed as a function of the master secret key K and the postal destination (See page 11, lines 7-12, for example).

In steps (e) and (f) the indicia is evidenced by using the computed verification key V_i^{Dest} to create a digital signature for the indicia, and digitally signing the indicia by including the digital signature and the computed key ID I_i^{Dest} on the indicia (See page

11, lines 14-17, for example). The mail piece bearing the postage indicia is now ready for mailing and subsequent verification.

VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claim 28 stands rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement.

Claim 28 stands rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 28-31 stand rejected under 35 U.S.C. §103 (a) as being unpatentable over U.S. Patent Application No. 5,812,666 to Baker et al. in view of U.S. patent 6,058,193 to Cordery et al.

VII ARGUMENTS

1. Rejection of Claim 28 under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement

In the Amendment dated June 7, 2006, Claim 28 was amended to recite that master secret key *K* and a secret key K_i are received by the PDGs "from a distribution center over a network after manufacture." The Remarks section of the Amendment stated,

> support for the amendment may be found throughout the specification, for example pages 1-3 and 6 -8. In particular, page 7, lines 3-5 describes the "…the key distribution center 24 distributes the cryptographic keys to the PGDs 14 and to the distribution centers 20 via a telecommunications network." Since FIG. 2 (and FIG.1 to which FIG. 2 is compared) show the PGDs 14 coupled between a distribution center and a distribution center, the distribution of the keys over the network clearly occurs after the PGDs have been manufactured.

In the Final Office Action dated March 7, 2006, the Examiner stated that "Applicants disclosure fails to recite receiving keys after manufacture. The specification, merely states the Key distribution center distributes cryptographic keys to the PGDs and to the distribution centers via a telecommunication network such as the Internet or private link (page 7)."

In rejecting a claim for a lack of written description, the Examiner must establish a prima facie case by providing reasons why a person skilled in the art at the time the application was filed would not have recognized that the inventor was in possession of the invention as claimed in view of the disclosure of the application is filed. (MPEP §2163 III. A. (Rev. 3, Aug. 2005, Page 2100-184)).

It is respectfully submitted that the Examiner has not established a prima facie case for a lack of written description because the Examiner failed to provide reasons

why a person skilled in the art of time the application was filed would not have recognized that the inventor was in possession of the invention as claimed in view of the disclosure. The only reason given by the Examiner is that "a transmission over a telecommunication network to a postage device does not equate that the transmission is after the transmission (sic) of the manufacturer of the device." (Final Office Action §1.1).

It is respectfully submitted, however, that a person of ordinary skill in the art at the time the application was filed would have recognized that the inventor was in possession of the invention as claimed in view of the disclosure. The Examiner appears to base his reason on a lack of explicit support in the disclosure for "after manufacture". However, a newly added claim limitation can be supported in the specification through express, implicit, or inherent disclosure. (MPEP §2163 I. B. (Rev. 3, Aug. 2005, Page 2100-175)).

It is respectfully submitted that the specification conveys with reasonable clarity to those with ordinary skill in the art that applicant was in possession of the invention as now claimed based on implicit and/or inherent support in the disclosure. FIGS. 1 and 2 of the specification show a prior art system and the system of the present invention, respectively, *in operation*, i.e., during the dispensing, evidencing and verification of the postage, which clearly occurs after the PGDs have been "manufactured". In light of the description in the disclosure, it is respectfully submitted that one of ordinary skill in the art would readily recognize that the Specification implicitly and/or inherently supports the fact that the cryptographic keys used by the PGD's 14 are received by the PGD's after the PGD's have been manufactured, since the PGDs are shown clearly delivered

and installed at user locations to evidence postage. As the specification fails to mention any embodiments where the Key distribution center delivers the keys to the PGDs during the manufacturing of the PGD's, no other interpretation is reasonable or supported.

Accordingly, the amendment made to Claim 28 is supported by the Specification as filed, and therefore complies with the written description requirement.

2. Rejection of Claim 28 under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention

In the Final Office Action dated March 7, 2006, the Examiner stated that the phrase "receiving... after manufacture" in claim 28 "renders the claim(s) indefinite because the claims(s) include(s) elements not actually disclosed. It is not clear what is being manufactured."

In response, Applicant points out the only item of manufacture in claim 28 on which the claim is based is the plurality of postage generating devices (PGDs). The preamble of claim 28 recites "a method for dispensing and evidencing postage indicia by a postage generating device (PGD) in a system having a plurality of PGDs that have been divided into n groups identified by a group designation G_i, i = 1,…n, the method performed by the indicia generating devices comprising." Step (a) then recites "receiving a master secret key... from a distribution center over a network after manufacture." From the preamble and the context of the claim, it is respectfully submitted that one of ordinary skill in the art would recognize that it is the PDG that is performing the "receiving" function, and that the receiving is performed after the PDG

has been manufactured. The preamble even states that it is the indicia generating devices that are performing the receiving. Also, when interpreted in light of the Specification, as discussed above, it is believed that one of ordinary skill in the art would find the claim language non-ambiguous as to the fact that the PDGs receive the keys from the distribution center after the PDG's have been manufactured.

Accordingly, Claim 28 is definite and particularly point out and distinctly claim the subject matter which applicant regards as the invention, and therefore complies 35 U.S.C. §112.

3. Rejection of Claim 28 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Application No. 5,812,666 to Baker et al. in view of U.S. patent 6,058,193 to Cordery et al.

No Prima Facie Case Of Obviousness

To establish a prima facie case of obviousness, three basic criteria must be met: the prior art reference must teach or suggest all the claim limitations, there must be a reasonable expectation of success, and there must be some suggestion or motivation to modify the reference or to combine reference teachings. MPEP §2142. It is respectfully submitted that a combination of Baker and Cordery fail to teach or suggest the combination of elements recited in independent claim 28, and that the Examiner's stated reason of suggestion or motivation to modify the reference or to combine the reference teachings is incorrect.

Baker provides a key management system that distributes cryptographic keys to digital meters for multiple domains, including vendor keys and postal keys for a plurality of countries. The key management system is configured to prevent translation of keys

between domains, to provide assurance in a domain that the keys were generated in the domain, and that each key has been installed in only one meter by the system (col. 3, lines 23-31). The key management system includes separate logical security domains: one vendor domain and or one more postal domains. Each domain provides a full set of key generation, key distribution, key installation and token verification services (col. 5, lines 24-27). Vendor data keys are generated at a vendor data center (col. 5, lines 42-54), and postal keys are generated at a postal data center (col. 6, lines 5-14).

Both vendor and postal master keys are installed in the digital meters (col. 6, lines 43-47), and each digital meter receives the vendor master key and postal master key while physically located in the vendor manufacturing facility before distribution (col. 6, lines 52-56). To enforce a security requirement that a master key can only be attempted or installed in any digital meter once, each master key is identified by a domain master key identification number (col. 7, lines 18-58). Domain keys are used to encrypt the domain master keys (vendor and postal) (col. 6, lines 61-63). The main keys are encrypted by domain Key set 103, which consist of a RSA key pair for confidentiality and an RSA key pair for authentication (col. 8, lines 4-15.)

In operation, each meter uses the domain master key to generate a temporal key, referred to as a token key for each domain, which is used to generate a token from mail piece data. Postal temporal keys distributed to postal verification sites are used for local verification of the indicia (col. 18, lines 23-34).

A. References Fail to Teach or Suggest All the Claim Limitations

It is respectfully submitted that the neither Baker or Cordery, singularly or in combination, teach or suggest the combination of elements recited in claim 28.

Referring to step (a), Baker fails to teach or suggest "receiving a master secret key *K* and a secret key K_i from a distribution center over a network after manufacture, and storing the master secret key *K* and the secret key K_i in the PGD," as recited in amended claim 28.

The Examiner cites column 6, lines 50-56 and column 9, lines 33-36 of Baker for disclosing the step. These passages, however, respectively state:

> A digital meter 36 receives the vendor master key and postal master key while physically located in the vendor manufacturing facility 14 **before distribution**, and
>
> The meter is securely configured so that **once keys are installed during manufacture**, they can never be removed or determined outside the manufacturing environment without leaving physical evidence of tampering.

Thus, Baker clearly teaches that the digital meters receive a vendor master key and postal master key *during manufacture* and before distribution. The teachings of Baker at column 16, line 30 through column 17, lines 4, which were cited by the Examiner, are also in the context of the manufacturing process. Accordingly, Baker fails to teach or suggest PGDs "receiving a master secret key *K* and a secret key K_i …over a network after manufacture," as recited in amended claim 28.

Referring to step (b) of claim 28, Baker does describe in the Background of the Invention the computer printing of postal indicia on the face of a mail piece (column 1). But Baker fails to teach generating an indicium "for a mail piece destined for a particular postal destination *Dest*," as recited in step (b), and then using the "*Dest*" to create a digital signature for the indicium as recited in steps (c)-(f) of claim 28, discussed below.

Referring to step (c) of claim 28, Baker fails to teach or suggest "computing a verification key V_i^{Dest} as a function of the secret key K_i and the postal destination." The Examiner cites column 5, lines 38-42 and column 17, lines 28-44 of Baker for teaching this step. However, these passages respectively state:

> The digital meter calculates two proof of payment tokens, one using the vendor master key and the other using the postal master key. Failure in the verification of either digital token is sufficient proof of fraud. Referring now to FIG. 3, vendor data center 12 provides physical and information access control for Key Management System components.
>
> Key registration consists of associating the country of registration, and the indicia number with the product code number and the key. The key is then stored in the country sub-domain of the install domain using a secret key that is specific to the country sub-domain. The essential feature is that the brass process that is specific to that country sub-domain relies on the install domain to install keys securely and with integrity. Keys never transfer from one install domain to another.
>
> Referring now to FIGS. 26 and 31, when the digital meter is prepared for a specific Security Domain, the Indicia Serial Number and/or Product Code Number is entered into the digital meter in message MR1. The PSR computer 34 requests registration tokens from digital meter 36 at 360. The digital meter generates two digital tokens and returns them the PSR computer at 362. The PSR computer combines the tokens with other meter information and forwards the…

These passages cited by the Examiner have nothing at all to do with "computing a verification key V_i^{Dest} as a function of the secret key K_i and the postal destination" and seem to be mistaken cites by the Examiner. Likewise, Baker also fails to teach or suggest the limitations of (d)-(f).

In the "Response to Arguments" section of the Office Action dated August 2, 2005, the Examiner responded to Applicant's previous argument that Baker does not teach verification key's generated as a function of the secret key and postal destination, and the verification keys are not used to create a digital signature, by citing the

Background of Baker. The Background of Baker teaches in general that in new digital meters, independent keys are used for generating digital tokens, and information about the meter and mail piece are combined and encrypted with vendor and postal master keys were keys derived therefrom (col. 2, lines 10-18). This discloses nothing more than what applicant disclosed in Applicant's Background of the invention, which states "when generating the IBI 22, the postage generating device 14 uses an internally generated private key and the public key to digitally sign the indicia, thereby creating a digital signature."

Applicant, however, is not attempting to claim the general notion of generating postage indicium with generated cryptographic keys. Instead, Claim 28 recites a specific implementation of computing keys to create a digital signature for indicia that is unobvious and has advantages over prior art approaches.

The present invention provides a method and system for dispensing and evidencing indicia by an indicia generating device in a system where a key distribution center divides the postage generating devices (PDGs) "into n groups identified by a group designation G_i, i = 1,...n", (Claim 28 preamble), which may be based on geographic designations (e.g., zip codes), and assigns a set of verification keys, V_i, to each PGD group, where each verification key in the set is encrypted as a function of one of the corresponding destination regions. The key distribution center also assigns a set of key ID's to each PDG group, where each key ID in the set is associated with one of the assigned verification keys and is encrypted as a function of the same destination region used to encrypt the corresponding verification key. After assigning the verification keys to the PGD groups, the KDC distributes to each distribution center

the sets of verification keys and key ID's that were encrypted as a function of the corresponding destination region.

The process begins when the PDG's receive a master secret key K and a secret key K_i from the KDC. In response to receiving a request from a user to generate an indicium for a mail piece destined for a particular destination *Dest*, the indicium is generated, and the verification key V_i^{Dest} is computed as a function of the secret key K_i and the destination. The PGD also computes the encrypted key ID I_i^{Dest} as a function of the destination. The PGD evidences the indicia in step by creating a digital signature for the indicia using the verification key V_i^{Dest} and digitally signs the indicia by including the digital signature and the computed index I_i^{Dest} on the indicia. The mail piece bearing the postage indicia is now ready for mailing and subsequent verification. These are the steps recited in claim 28.

None of Baker's disclosed keys teach or suggest the keys and functionality of the keys described above and as recited in claim 28. For example, it is noted Baker discloses that a domain maser key is installed in each meter, and that each meter uses the domain master key to generate a temporal key, referred to as a token key, for each domain, which is used to generate a token from mail piece data. However, it is not believed either Baker's master key or the temporal key is analogous to the verification key.

Baker's master key is not analogous because it is installed during manufacturing, not received by the PGD "over a network after manufacturing." Because the domain master key is already present in the meter, it is also not computed as a function of "a secret key" and the postal destination, as required by step (c). The

domain master key is also not used "to create a digital signature for the indicia", as recited in step (e). Instead, Baker's temporal key is used to generate the token from mail piece data. In addition, although Baker may teach that earth domain digital meters are assigned a country specific security domain and receive copies of earth domain master keys that are encrypted with a country specific secret key, Baker fails to teach or suggest that meters in each group designation, "G_i, i = 1,…n", also receive "a secret K_i,", which corresponds to that Group designation via the i = 1,…n, as required by step (a).

It is believed Baker's temporal key is not analogous to the claimed verification key because although the temporal key is computed from one key (the domain master key), it is not computed as a function of a second key, the "secret key", and the postal destination, as required by step (c).

Moreover, it is believed that Baker's country specific secret keys cannot be considered analogous to the recited secret K_i because Baker's country specific secret keys are not believed to be installed in the meters. In addition, Baker's country specific secret keys are not used by the meters to "comput[e] a verification key V_i^{Dest} as a function of the secret key K_i and the postal destination (*Dest*), as recited in step (c).

The Examiner relies on Cordery et al to cure the deficiencies of Baker. Cordery may teach the storing of a postal master key and a vendor master key in a meter and using the postal and vendor master keys to generate in the meter respective postal and vendor token keys that are then used to generate respective unique postal and vendor tokens that are date dependent. However, in Cordery there is no dividing the meters into groups. Therefore, there can be no distributing a master secret key K and a secret

key K_i to the PGDs in the groups G_i, $i = 1,\ldots n$, which in turn means there can be no "computing a verification key V_i^{Dest} as a function of the secret key K_i" and using the verification key to create a digital signature for the indicia.

B. Incorrect Motivation to Combine

In addition to the fact that a combination of Baker and Cordery fail to teach or suggest all the limitations of claim 28, it is respectfully submitted that the Examiner also fails to state a prima facie case of obviousness because the motivation to combine the references stated by the Examiner is incorrect.

The Examiner stated "it would have been obvious to of ordinary skill in the art at the time the invention was made to modify the method of Baker et al. to use the generated verification key to create digital signature for the indicia, and digitally signing [sic] the indicia by including the digital signature and other generated token[sic] on the indicia because it would allow other party[sic] to determine whether both keys can be trusted that they actually originate from the meter." Office Action page 5.

The present invention, however, provides an improved method for evidencing and verifying postage indicia in which postage validation is performed at destination distribution centers, rather than at originating distribution centers, and the verification keys, which are encrypted as a function of the destination, are only distributed to the corresponding distribution centers. Thus, even if a destination center were broken into, the perpetrator would only be able to forge postal indicia for mail pieces destined for the particular destination. In addition, the key ID is also encrypted so that even if a perpetrator were to crack a verification key, the perpetrator would still have a problem

identifying which verification key was obtained. In order to forge the indicia, the perpetrator must possess two keys, rather than one, a secret key that the PGD used to compute the key ID, and the verification key itself.

The Examiner's stated motivation to determine whether both keys can be trusted that they actually originate from the meter has nothing to do with increasing security of the evidencing and verifying postage indicia in the manner claimed.

Accordingly, Appellant respectfully requests withdrawal of the rejection under 35 U.S.C. 112 and 103(a) and respectfully requests that the Board reverse the final rejection of Claims 28-31.

For all the foregoing reasons, it is respectfully submitted that Claims 28-31 (all the Claims presently in the application) are patentable. Thus, Appellant respectfully requests that the Board reverse the rejection of all the appealed Claims and find each of these Claims allowable.

Note: For convenience of detachment without disturbing the integrity of the remainder of pages of this Appeal Brief, Appellant's "APPENDIX" sections are contained on separate sheets following the signatory portion of this Appeal Brief.

Respectfully submitted,
STRATEGIC PATENT GROUP

November 3, 2006
Date

/Stephen G. Sullivan/
Stephen G. Sullivan
Attorney for Appellant(s)
Reg. No. 38,329
(650) 493-4540

VIII CLAIMS APPENDIX

28 (Previously Presented) A method for dispensing and evidencing postage indicia by a postage generating device (PGD) in a system having a plurality of PGDs that have been divided into n groups identified by a group designation G_i, $i = 1,\ldots n$, the method performed by the indicia generating devices comprising:

(a) receiving a master secret key K and a secret key K_i from a distribution center over a network after manufacture, and storing the master secret key K and the secret key K_i in the PGD;

(b) in response to receiving a request to generate an indicium for a mail piece destined for a particular postal destination *Dest*, generating the indicium;

(c) computing a verification key V_i^{Dest} as a function of the secret key K_i and the postal destination;

(d) computing a key ID I_i^{Dest} as a function of the master secret key K and the postal destination;

(e) using the computed verification key V_i^{Dest} to create a digital signature for the indicia; and

(f) digitally signing the indicia by including the digital signature and the computed key ID I_i^{Dest} on the indicia.

29 (Original) The method of claim 28 further including the step of computing each verification key V_i^{Dest} as a one-way function H of the PGD group key K_i and a designation of the postal destination:

$$V_i^{Dest} = H(K_i, Dest).$$

30 (Original) The method of claim 29 further including the step of using ZIP codes to designate the postal destination.

31 (Original) The method of claim 30 further including the step of computing each of the key ID's as a one-way function *H* of the PGD group, G_i, the master secret key, *K*, and a designation of the postal destination, *Dest*:

IX EVIDENCE APPENDIX

(None)

X RELATED PROCEEDINGS APPENDIX

(None)